UNIVERSITI SAINS MALAYSIA

Second Semester Examination
Academic Session 1998/99

February 1999

CSC535 - Cryptography

Duration : [3 hours]

INSTRUCTION TO CANDIDATE:

- Please ensure that this examination paper contains **FIVE** questions in SIX printed pages before you start the examination.
- Answer any **FOUR** out of five questions. Each question is worth 25 points for a . possible total of 100 points.
- Some questions may depend (directly or indirectly) on others for a complete solution. It is suggested that you read all questions before deciding on-which to attempt.
- Show any appropriate intermediate work, this might result in partial credit (if solution method is correct) even if the final answer is incorrect.
- Use of scientific or programmable calculator is permitted.
- Notes written on a single sheet of A4 paper may be brought in and used. Any other written notes or publications are disallowed.
- Questions may be answered either in Bahasa Malaysia or English.

---

1. (a) Give an algorithmic description for Greatest Common Divisor (GCD) determination using Euclid's method. Assume that the function will be called Euclid(p, q) with $p < q$.

(4/25)

(b) State the algebraic property associated with x^{-1} ie the multiplicative inverse modulo(n). When is x^{-1} guaranteed to exist? Show that solving for a multiplicative inverse is equivalent to solving the equation $ax + bn = 1$ in which {x, n} are known and {a, b} unknown.

(3/25)

(c) Give an algorithmic description for multiplicative inverse determination using an extension of Euclid's method. Provide a sound argument as to which parameter should be associated with the multiplicative inverse.

Explain how this algorithm can be straightforwardly extended to solve equations of form $\sum_i a_i x_i = 1$ in which all $\{x_i\}$ are known and all $\{a_i\}$ are unknown.

(8/25)

(d) State the Chinese Remainder Theorem (CRT). Demonstrate that any modular basis can always be decomposed into factors which are pairwise relatively prime.

(3/25)

(e) Show that sub-modular decomposition as prescribed in the CRT is well-defined and invertible, and that the usual rules of modular arithmetic applies to the individual components.

(7/25)

2. (a) Sketch out the block-structure of the non-linear round function for the International Data Encryption Algorithm (IDEA). Explain in terms of number theory how multiplication provides "confusion" to the plaintext-to-ciphertext translation process.

A generalisation of IDEA with operations:

$$A + B = A + B \bmod(2^n)$$
$$A \oplus B = \text{Xor}(A, B)$$
$$A * B = A * B \bmod(2^n + 1)$$

for $n \in \{2, 4, 8\}$ can be derived straightforwardly from basic (n = 16) IDEA, but not the n = 32 case. Explain the significance of the moduli basis for the + and * operations.

(5/25)

(b) Consider (n = 8) IDEA. Explain how 8-bit (double-hex) words can be used to represent elements in the multiplicative group modulo(FF + 2).

Show the block-structure for a single round of reduced IDEA computation.

Indicate bit-widths for all intermediate variables. In all cases; use notation $X_k^{(i)}$ in which the superscript index indicates the i-th computational round, and the subscript index indicates ordering within that particular round.

Specify all necessary modifications in (a), then repeat this procedure for the final output transformation stage. What is the block-size for (n = 8) IDEA?

(7/25)

(c) Consider (n = 8) IDEA with 2 rounds of computation. Using similar notation as in (b), list out all subkeys required. What is the subkey bit-width?

Present a modification of the IDEA subkey generation routine so as to be able to generate all necessary subkeys. Start with a 64-bit key and execute 13-bit shifts between subkey generation rounds. Why are these particular values significant?

(5/25)

(d) Use key K = 71EC A15C 6655 BC3B given in hex representation. Calculate all required subkeys.

(4/25)

(e) Calculate the resultant ciphertext for plaintext block P = 86B8 DFBB D368 9089.

Use Cipher Block Chaining (CBC) with null initialisation. Why is this operational mode considered more secure than Electronic Codebook (ECB) mode?

(4/25)

3. (a) Demonstrate how a binary representation of the exponent and the rules of modular multiplication can be used to simplify expressions of form A^k mod p.

Give an algorithmic description of how such expressions can be evaluated.

(6/25)

(b) An implementation of the El-Gamal public-key cryptosystem uses the following numbers as system parameters:

p = FF+2 = 101	as the modular basis
g = 4B	as the generator

A new user generates random secret-key x = E9. Calculate the public-key associated with x, representing all numbers as 8-bit (double-hex) words.

(5/25)

(c) Sketch out the computational details of El-Gamal encryption and decryption. Explain how prior possession of the private-key is essential for successful decryption.

(6/25)

(d) Calculate the ciphertext resulting from plaintext M = 48.

(4/25)

(e) Demonstrate plaintext recovery from the ciphertext generated in (d). Why is this operation always guaranteed to work?

(4/25)

4. (a) Sketch out the block-structure of a generic compression step within the Message Digest (MD) 5 hash function. Make the modifications necessary to accommodate 64-bit width chain variables and 128-bit message chunks. Retain the $V_q = (a, b, c, d)_q$ structure of the chain variable, but modify all other system parameters as you deem appropriate.

(6/25)

(b) Use F_3 and ρ_1 ie the logical function and index permutation usually associated with the 3rd and 1st rounds in MD5, and the following additive constants:

i	T[i]
1	269C
2	8E17
3	F034
4	91E7
5	0B57
6	124B
7	8171
8	FCD5

Execute a single computational round to generate V_{q+1} given the following input parameters:

V_q = 628E 2525 6228 B969 as the chain variable
M_q = 5FA4 B5AB 3693 0614 EE74 190A 0818 1CAD as the message chunk.

(5/25)

(c) Symmetric block ciphers are sometimes used to implement iterated hash functions, with V_q as the plaintext and V_{q+1} as the ciphertext. Such schemes commonly feature equal-sized chain variables and message chunks. You are required to implement such a hash function using IDEA as the block cipher. Describe your hashing scheme in terms of a block diagramme or recurrence relation.

(6/25)

(d) Compare block-cipher based hashing as developed in (c) to the more usual compression-based hashing ie MD5 or the Secure Hash Algorithm (SHA) in terms of:

- Speed ie hashing bit-rate
- Security ie non-invertibility and collision protection

(4/25)

(e) Describe—by listing all appropriate steps—an attack on Rivest-Shamir-Adleman (RSA) signatures in which encrypted messages can be intercepted, manipulated and subsequently compromised.

How does using a hash function prior to signature generation prevent such an attack?

(4/25)

5. (a) RSA-based anonymous digital cash requires that an identity string (I) be "divided" into left and right halves. How is this done? Why is the pair (I_L, I_R) referred to as a split secret?

(4/25)

(b) Explain the general concept of a blind signature. Describe—by listing all appropriate steps—how a subsequently verifiable signature can be affixed on a "blinded" document initially not visible to the signer.

Why does blinding-unblinding commute with RSA encryption-decryption?

(6/25)

(c) Specify the information required in a Coin data structure, then describe the Customer-Bank handshake sequence needed to create an anonymous Coin with a verifiable Bank signature.

What information in the coin data structure cannot be revealed to the Bank in order to preserve anonymity?

(6/25)

(d) Note that the blinding procedure in (b) requires direct signature affixation on the application data ie the Coin. Performance and library-support considerations would also dictate signature affixation on a hash value. Explain how a hash function might be used within the context of Coin creation in (c), and suggest a data exchange sequence which would lead to an improvement in operational efficiency.

(5/25)

(e) Explain how single usage of a Coin allows the Customer to remain anonymous, while multiple usage of the same Coin results in the Customer being identified.

How is Vendor-perpetrated fraud detectable from Customer-perpetrated fraud?

(4/25)

- oooOOooo -